UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,487	08/16/2001	Edward W. Kohler JR.	12221-006001	3664

26161 7590 06/17/2005

FISH & RICHARDSON PC
225 FRANKLIN ST
BOSTON, MA 02110

EXAMINER
ISMAIL, SHAWKI SAIF

ART UNIT	PAPER NUMBER
2155	

DATE MAILED: 06/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,487	KOHLER ET AL.	
	Examiner	Art Unit	
	Shawki S. Ismail	2155	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 March 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

RESPONSE TO AMENDMENT

1. This communication is responsive to amendment filed on March 14, 2005. Applicant amended claims 1, 2, 3, 15, and 20, and added new claims 21-32. Claims 1-32 remain for further examination. Applicants' arguments with respect to claims 1-20 have been fully considered.

The New Grounds of Rejection

2. Applicants' amendment and arguments with respect to claims 1-20 filed on March 14, 2005 have been fully considered but they are deemed to be moot in view of the new grounds of rejection.

Drawings

3. Examiner acknowledges receipt of the amendment to the specification, which overcomes the objection to the drawings made in the last Office Action, mailed January 19, 2005.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having

ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-12, 15-32, are rejected under 35 U.S.C. 103(a) as being unpatentable over **Cox et al.,** (Cox) U.S. Patent No. **6,738,814** and in view of **Vaidya** U.S. Patent No. **6,279,113.**

6. As to claim 1, Cox teaches a method of protecting a victim site against a denial of service attack, the method comprises:

receiving from the victim site a notification that the victim site is under an attack (col. 3,. Lines 23-29, the routing device is located on the site of the victim therefore it notifies the system administrator that an attack has taken place); and

Cox does not explicitly teach sending queries to data collectors, deployed at different points in a network that carries network traffic to the victim site, that sample network packets and collect statistical information on network packets sent over the network, to request the statistical information from at least some of the data collectors, the statistical information to determine the source of suspicious network traffic heir sent to the victim data center.

Vaidya teaches detecting intrusion attempts into system resources by monitoring for attack signature. Vaidya teaches that multiple data collectors each of which includes a data monitoring device, man attack signature profile memory, and a processor are deployed at multiple sites in different segments of the network. Statistical analysis associated with an attack signature are kept in a signature profile memory and

accessed by the data collectors in order to determine if the packet is associated with a network intrusion (col. 3, lines 49-65, col. 6, line 57 – col. 7, line 10).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the teaching of Vaidya into the invention of Cox in order to maintain a statistical information on network packets in order to easily and efficiently determine network intrusion and be able to better to diagnose it.

7. As to claim 2, Cox teaches the method of claim 1 wherein the network packets from the attacker have faked, random source addresses that change with time (col. 3, lines 55-56). Cox does not explicitly teach wherein sending queries to data collectors for the statistical information is based on victim destination address.

Vaidya teaches sending queries to the data collectors for the statistical information based on victim destination address (col. 3, lines 49-65, col. 6, line 57 – col. 7, line 10).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the teaching of Vaidya into the invention of Cox in order to get the right statistical information. Each data collector is deployed at different segments of the network. Therefore, the system needs to know the victims destination address in order to be able to contact the data collector for associated with that victim.

8. As to claim 3, Cox teaches the method of claim 1 as discussed above. Cox does not explicitly teach wherein based on collected statistical information the method further comprises determining what data centers are performing the spoofing on the victim.

Vaidya teaches determining what data centers are performing the spoofing on the victim (col. 3, lines 49-65).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the teaching of Vaidya into the invention of Cox in order to maintain system manageability. By knowing what data centers or data collectors are performing the diagnosis and analysis on the victim will give the system better control on the network.

9. As to claim 4, Cox teaches the method of claim 3 wherein determining is performed by a control center, and determining further comprising: sending data to/from a gateway device that is associated with the victim center (col. 3, line 55 – col. 4, line 15).

10. As to claim 5, Cox teaches the method of claim 4 wherein the gateway identifies the network address of the victim, via a message to the control center (col. 4, lines 41-61).

11. As to claim 6, Cox teaches the method of claim 5 wherein the message is sent over a hardened network (col. 4, lines 41-61).

12. As to claim 7, Cox teaches the method of claim 5 wherein message indicates the type of attack (col. 3, lines 35-45 and col. 4, lines 41-61).

13. As to claim 8, Cox teaches the method of claim 1 wherein the attacker is behind a gateway (col. 3, line 55 – col. 4, line 15).

14. As to claim 9, Cox teaches the method of claim 8 wherein if the attacker is behind a gateway, the control center issues a request to the gateway that the attacker is behind to block the attacking traffic (col. 3, line 55 – col. 4, line 15).

15. As to claim 10, Cox teaches the method of claim 8 wherein if the attacker is behind a gateway, the gateway that the attacker is behind selectively discards traffic that appears to be malicious traffic and that contains the victim destination address (col. 3, line 55 – col. 4, line 15).

16. As to claim 11, Cox teaches the method of claim 1 wherein if the attacker is not behind a gateway, the control center queries the data collectors to provide information about possible locations of the attackers (col. 3, line 55 – col. 4, line 15).

17. As to claim 12, Cox teaches the method of claim 1 wherein if the attacker is not behind a gateway, the method further comprises:

contacting administrators at locations involved in attack to have the administrators take action to filter out packets with the destination address (col. 4, lines 10-15).

18. As to claim 15, Cox teaches a method of protecting a victim site against a denial of service attack, the method comprises:

receiving packets with faked, random source addresses (col. 3, lines 55-56);

receiving, from a gateway disposed near the victim site, a notification that the victim data center is under an attack (col. 3,. Lines 23-29, the routing device is located on the site of the victim therefore it notifies the system administrator that an attack has taken place); and

Cox does not explicitly teach sending queries to data collectors deployed at different points in a network that carries network traffic to the victim site, that sample network packets and collect statistical information on network packets sent over the network to request statistical information from data collectors that have examined network traffic with the victim destination address.

Vaidya teaches detecting intrusion attempts into system resources by monitoring for attack signature. Vaidya teaches that multiple data collectors each of which includes a data monitoring device, man attack signature profile memory, and a processor are deployed at multiple sites in different segments of the network. Statistical analysis associated with an attack signature are kept in a signature profile memory and accessed by the data collectors in order to determine if the packet is associated with a network intrusion (col. 3, lines 49-65, col. 6, line 57 – col. 7, line 10).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the teaching of Vaidya into the invention of Cox in order to maintain a statistical information on network packets in order to easily and efficiently determine network intrusion and be able to better to diagnose it.

19. As to claim 16, Cox teaches the method of claim 15 wherein the control center also includes a communication process to send data to/from a gateway device that is disposed with the victim center (col. 4, lines 41-61).

20. As to claim 17, Cox teaches the method of claim 16 wherein if the attacker is behind a gateway, the control center issues a request to the gateway to block the attacking traffic (col. 3, line 55 – col. 4, line 15).

21. As to claim 18, Cox teaches the method of claim 17 wherein if the attacker is behind a gateway, the gateway selectively discards traffic that appears to be malicious traffic and that contains the victim destination address (col. 3, line 55 – col. 4, line 15).

22. As to claim 19, Cox teaches the method of claim 15 wherein if the attacker is not behind a gateway, the method comprises:

contacting administrators at locations involved in attack to filter out packets having the destination address (col. 4, lines 10-15).

23. Claims 20-32 are essentially the system and computer program of the method of claim 1; therefore they are rejected under the same rationale.

24. Claim 13 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Cox et al.,** (Cox) U.S Patent No. **6,738,814** and in view of **Hill et al.,** (Hill) U.S. Patent No. **6,088,804.**

25. As to claim 13 and 14, Cox teaches a method for blocking denial of service and address spoofing attacks on a network. However, Cox does not explicitly teach wherein the attacks are classified into categories based on the severity that they cause to the network.

Hill teaches a system and method for adaptively responding to computer network security attacks. Hill further teaches classifying attacks based on the severity of the attack on the network (Fig. 3, col. 2; lines 53-60; col. 6, lines 9-22).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate Hill's classification of the severity of attacks into the invention of Cox in order minimize the load on the computer network. Displaying attack

information would help the network manager prioritize the severity of the attacks so that it spend less time countering lesser threats and more time countering severe threats (col. 2, lines 47-53).

26. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shawki S Ismail whose telephone number is 571-272-3985. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on 571-272-4001. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shawki Ismail
Patent Examiner
June 12, 2005

SALEH NAJJAR
PRIMARY EXAMINER